19th ICCRTS

"C2 Agility: Lessons Learned from Research and Operations."

Practical Considerations for Use of Mobile Apps at the Tactical Edge

Primary Topic: Cyberspace, Communications, and Information Networks
Alternate Topic 1: Social Media
Alternate Topic 2: Data Information and Knowledge

Paper Number 035

Jonathan R. Agre
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311, USA
+1-703-933-6522
jagre@ida.org

Karen D. Gordon
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311, USA
+1-703-845-2343
kgordon@ida.org

Marius S. Vassiliou
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311, USA
+1-703-887-8189
+1-703-845-4385
mvassili@ida.org

Point of Contact:
Jonathan R. Agre
Institute for Defense Analyses
4850 Mark Center Drive
Alexandria, VA 22311-1882, USA
703-933-6522
jagre@ida.org

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2014		**00-00-2014 to 00-00-2014**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Practical Considerations for Use of Mobile Apps at the Tactical Edge	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Institute for Defense Analyses,4850 Mark Center Drive,Alexandria,VA,22311**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

Presented at the 18th International Command & Control Research & Technology Symposium (ICCRTS) held 16-19 June, 2014 in Alexandria, VA. U.S. Government or Federal Rights License

14. ABSTRACT

Along with the increased interest by the U.S. Department of Defense (DoD) in the use of portable electronics for the warfighter as part of the Command and Control (C2) infrastructure, such as smart phones and tablet computers, there is the alluring possibility of incorporating or adapting the associated commercial mobile apps ecosystem to gain access to the vast array of functionality available. Currently, over a million Android apps and a million iOS apps are available for download from the Google Play and Apple iTunes app stores, respectively. Of these, most would not be considered relevant to the military mission in their original forms, but often can form the basis of militarily useful functions after suitable customization (e.g., social media for C2, games adapted for training, maps for situational awareness). In addition, due to the special requirements of the military environment at the tactical edge, there are serious practical considerations that need to be addressed, such as operating under limited communications and establishing a viable app ecosystem, in order to successfully tap into these apps. The commercial mobile app ecosystem requirements, features and enablers are compared with the military environment. Key factors to be considered include major differences in the economic drivers and scale between the commercial world and DoD for developers and deployers, the increased security needs of the apps for soldiers both from the vulnerability and supply-chain aspects, difficulties in patching and keeping platforms and apps up-to-date, privacy constraints, and concerns about the distribution of information such as location data. The DoD is currently pursuing several policy, research and pilot efforts, primarily at the enterprise level versus the tactical edge, to facilitate implementation of some form of mobile apps ecosystem. However, there remain many significant research challenges and possible strategic directions that can be followed to better take advantage of the booming commercial mobile app ecosystem.

15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**35**	

Abstract

Along with the increased interest by the U.S. Department of Defense (DoD) in the use of portable electronics for the warfighter as part of the Command and Control (C2) infrastructure, such as smart phones and tablet computers, there is the alluring possibility of incorporating or adapting the associated commercial mobile apps ecosystem to gain access to the vast array of functionality available. Currently, over a million Android apps and a million iOS apps are available for download from the Google Play and Apple iTunes app stores, respectively. Of these, most would not be considered relevant to the military mission in their original forms, but often can form the basis of militarily useful functions after suitable customization (e.g., social media for C2, games adapted for training, maps for situational awareness). In addition, due to the special requirements of the military environment at the tactical edge, there are serious practical considerations that need to be addressed, such as operating under limited communications and establishing a viable app ecosystem, in order to successfully tap into these apps. The commercial mobile app ecosystem requirements, features and enablers are compared with the military environment. Key factors to be considered include major differences in the economic drivers and scale between the commercial world and DoD for developers and deployers, the increased security needs of the apps for soldiers both from the vulnerability and supply-chain aspects, difficulties in patching and keeping platforms and apps up-to-date, privacy constraints, and concerns about the distribution of information such as location data. The DoD is currently pursuing several policy, research and pilot efforts, primarily at the enterprise level versus the tactical edge, to facilitate implementation of some form of mobile apps ecosystem. However, there remain many significant research challenges and possible strategic directions that can be followed to better take advantage of the booming commercial mobile app ecosystem.

Keywords—*mobile apps, app ecosystem, app store, tactical edge*

1 Introduction

The U.S. Department of Defense (DoD) is increasingly interested in the use of commercial portable electronics for the warfighter, such as smart phones and tablet computers, for many reasons, including their familiarity to soldiers, their compact size, and their ability to execute a myriad of useful mobile apps (i.e., applications) [1]. There is the tantalizing possibility of incorporating or adapting the associated commercial mobile apps ecosystem for military purposes in order to gain access to the vast array of functionality available.

The explosive rise of the mobile app market started with the introduction of the Apple iTunes app store in 2008 coupled with the powerful iPhone user interface and integrated iTunes billing. In the first quarter of 2013, there were more smartphones sold than conventional feature phones for the first time,

with 51% of 418.6 million units [2]. The number of Android apps available in the Google Play app store surpassed one million in July 2013 [3], and the number of iOS apps in the Apple iTunes app store surpassed one million in October 2013 [4]. There are many types of mobile apps and most would not be considered relevant to the military mission, but they often can be viewed as forming the basis for a militarily useful function after suitable customization (e.g., games adapted for training).

The commercial mobile apps exist in an ecosystem that both supports and drives the diversity of apps available on the market, including support of the development and deployment of the apps, as well the infrastructure that enables them to operate. However, there are important differences between the tactical military environment and the commercial world that inhibits the direct adaptation of this ecosystem for military purposes. For example, mobile apps typically assume there is a viable communications infrastructure in which to operate, but the tactical edge is often operating under disconnected, intermittent, and limited (DIL) communications. Other key differences include the economic drivers, the scale in terms of users and developers, the increased security needs of the apps for soldiers, and concerns about the distribution of sensitive information such as location data.

The DoD has made several initial efforts at understanding and implementing mobile app environments, primarily at the enterprise level versus the tactical edge, together with experimentation on adoption of mobile devices. Important lessons have been learned; however, there remain significant research challenges and possible strategic directions that can be followed to better take advantage of the booming commercial mobile apps ecosystem.

In this paper, we describe the various types of mobile apps and the mobile apps ecosystem. Important differences between the commercial world and the military environment and some of the military-specific requirements are discussed. Several efforts of the DoD to utilize mobile apps and to build an ecosystem are summarized, and lessons learned are pointed out. Lastly, several technology gaps and research areas which hold promise for the future are identified.

2 Mobile Apps and Their Ecosystems

Mobile apps are defined as software applications that are downloadable to a mobile device, such as a smartphone or a tablet, and that can execute on those devices in either a stand-alone fashion or through a browser. They are designed to operate within the constraints of those platforms, including limited processing, display, memory resources, and battery life. They are typically limited in functionality but can take advantage of services hosted at remote data centers with requests/results delivered through the network. Mobile apps can be implemented in two forms: as native apps or as web-based applications. Most apps are built as native apps using the functionality on the device, while the web-based apps use the device browser.

Mobile apps can be organized in various ways. In iTunes, apps are grouped into the types shown in Figure 1 [5]. Of the more than 1.1 million apps represented, the most common apps include games and other apps of limited capability, such as Flashlight (second most popular free iPhone app in the utility category, right behind Find My iPhone [6]). Interestingly, apps such as productivity tools, navigation,

weather, and social networking each account for under 3%. Many of the apps interact with remote sites in useful ways (e.g., mapping and other location-based services) that incorporate more of the user's context. Other popular apps provide an interface to remote data sources, such as Google search or Facebook versus those supporting on-board functions. These basically customize the familiar desktop experience on the mobile device.

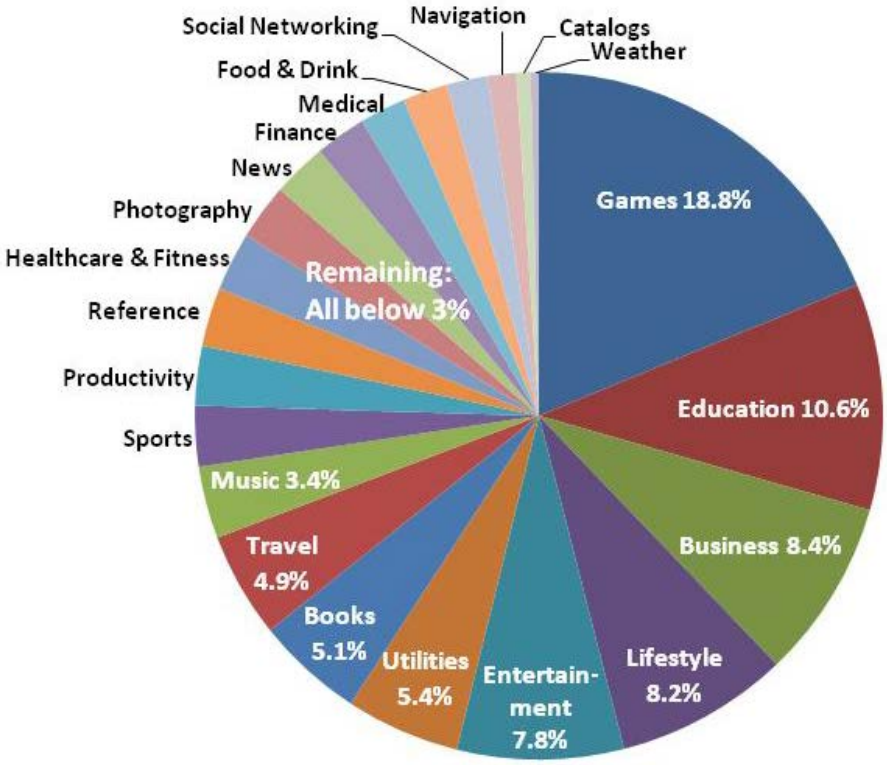


Figure 1: Categories of Mobile Apps in the iTunes App Store [4]

The proliferation of mobile apps has resulted in a new collection of processes and entities—the mobile apps ecosystem. The mobile apps ecosystem consists of a micro and macro ecosystem as shown in Figure 2. The micro ecosystem focuses on the deployment of the app store. The macro ecosystem is the infrastructure in which the developers, users, and micro ecosystem exist; it includes the mobile devices, networks, servers, and data storage facilities.

A. The Micro Ecosystem

The micro ecosystem includes all of the activities associated with the business of selling and delivering applications to smart phones and tablet computers, typically through an app store accessible through a network. The typical stages of the micro ecosystem [7] can be viewed as:

- Support for the development of the app
- Verification and validation (V&V) (or vetting) by the distributor
- Deployment of the app in an app store (owned by the distributor) for sale and distribution

- Support for the sustainment of the mobile apps

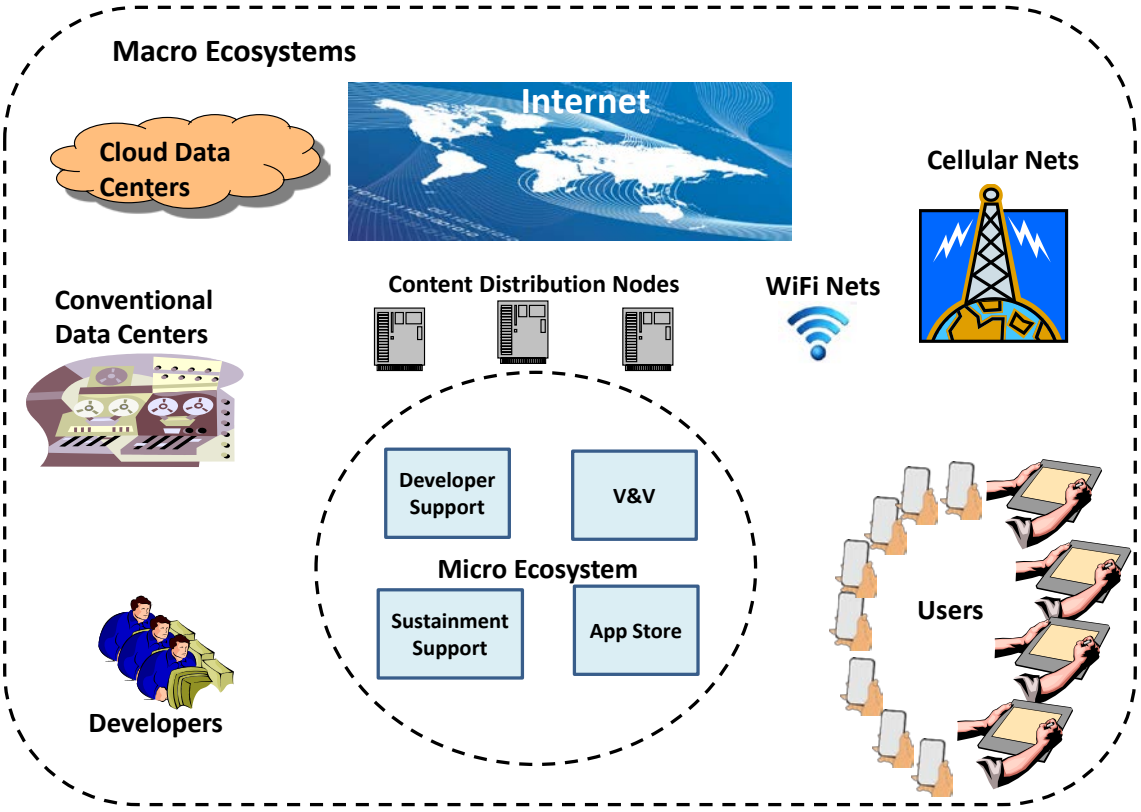


Figure 2: The Commercial Mobile App Ecosystem: Micro and Macro

The following discussion mainly deals with native apps, since web apps may provide some of these functions on their own web servers.

Development Support. Apps can be independently developed or contracted for by a distributor. A distributor will provide support for the developers, usually for a fee (e.g., $99 from iTunes and $25 from GooglePlay). In return for this fee, the app store will provide services helpful to the developer such as "shelf space," promotions, system development kits (SDKs), management tools, device catalogs, utility functions, graphics, application statistics, and ratings. For the Apple products, drivers of specific features of their devices are available in the app store, but, in the Android OS world, the situation is more complex due to the separation of the many device manufacturers and the operating system provider (i.e., Google). Sometimes the cellular carrier is also involved for carrier-specific operations.

V&V. Once an app has been completed, the app is delivered to the distributor for verification and validation, also called vetting. This typically requires a team of experts that can perform functional unit testing on the various devices and versions, integration testing, security, compliance verification, usability, and other criteria imposed by the app store (e.g., copyright violations, pornography, political correctness, etc.). When vetting is completed, the app is transitioned to the public access portion of the app store.

App Store Deployment. A distributor's app store is typically implemented in a private data center accessible to the users via an app (e.g., the built-in App Store app for accessing iTunes) that runs on the user's mobile device. The app allows the user to view information about the collection of apps available and to select, purchase, and download an app. The main functions of the app store include:

- Secure and efficient hosting of apps and support of downloads
- Identification of the user platform and delivery of the correct version of the app
- Authentication and access control of the users requesting downloads
- Attestation of the app and any updates (verification that the app has not been unexpectedly modified)
- Support of updates and maintenance functions
- Display of the apps, along with user reviews and ratings for each app, for enhanced app discovery
- Support of accounting functions such as purchasing and logging

The commercial app stores must scale to very large numbers of users (e.g., iTunes has over 800 million accounts, most with credit cards [7]. Authentication procedures and associated access control mechanisms may vary from account-name-password methods to more sophisticated methods, such as two-factor or biometrics, and support secure credit-card based transactions. Many app stores support single-sign-on from recognized business partners, such as Google+.

Sustainment. The app store will host updates to the apps and notify users of pending updates. Mechanisms to allow users to enter feedback and ratings on the apps are collected and displayed, as well as to provide additional useful statistics on the number of downloads, rankings, sales, etc. Accounting functions are provided for the financial and auditing functions necessary for sales and distribution.

B. The Macro Ecosystem

The macro, or umbrella, ecosystem is the enabling infrastructure to support the user experience and to enable the developers to efficiently create apps that interact with the global information resources.

Networks. In the commercial world, sufficient communications is available to support the downloading and updating of the apps, as well as the data access and transfer needs of the apps. Recent improvements to the networks are yielding benefits to the mobile apps ecosystem, including new streaming technologies for mobile video, and content delivery systems reducing latency and further increasing availability.

User Devices. The computational power, storage, and battery life of mobile devices continue to improve, enabling more powerful apps. Multi-mode communication is available to access the various types of networks and increase connectivity options. Various embedded sensors, such as cameras, GPS, and accelerometers, have spawned apps that take advantage of the local resources (e.g., photography apps, location information).

Computing Facilities. The macro ecosystem also includes the data centers that host the servers and the storage facilities necessary for the functioning of the apps. The rise of cloud computing and web services

has facilitated the rapid development of mobile apps as well as supported the relative ease in accessing remote data. Developers can use the elastic, on-demand provisioning of hardware in a cloud environment to reduce the investment needed to launch an app. In addition, as more data is placed in the cloud, mobile apps have been quick to take advantage of this trend to provide useful functions, such as through mashups (apps created by combining data or functionality using various available data sources).

Developers. Mobile apps are being developed in a fundamentally different manner than traditional software development activities [9]. Mobile Apps are spawned quickly with limited functionality, intended to deliver the most useful capability in a simple package. The product is evolved through a series of updates to increase market share or to keep up with the competitors. User feedback is quickly returned to the developer through the app store so that problems and complaints can be quickly addressed. This development pace is substantially faster than in the past, and the traditional software development waterfall model is not used as it consumes too much time and resources.

Native apps currently provide better performance and access to the device's capabilities, while web-based apps offer portability and are cheaper to develop. On the software side, the two most popular languages are Java for Android platforms and Objective C for Apple iOS devices. One trend is the increasing adoption of HTML5 as the delivery language for web-based data and services. It is estimated that there are now 1.4 billion mobile devices capable of operating with HTML5 [10]. HTML5 has a mode that uses locally cached data to continue limited operations when disconnected from the network.

C. App Ecosystem Drivers

The success of mobile apps is largely due to the mass market for the products. Statistics for iOS are shown below in Table 1 [4] [5][7][11] [12] [13]. Android statistics are similar.

The app ecosystem is driven in part by the sales of apps, in which a portion of the sales goes to the distributor and the rest to the developer. For example, the iTunes app store will collect 30% of the sales price of an app [14].

Table 1: Apple iTunes App Store Mass Market

iPhones sold	**500 million**
iOS devices sold	**800 million**
active iTunes accounts	**800 million**
countries represented	**155**
active iOS apps	**1.1 million**
iOS downloads	**60 billion**
registered iOS developers	**300,000**
payments to iOS developers	**$13 billion**

There are many apps that are free or very low in cost (e.g., $0.99 to $1.99). These apps are often:

- Not-monetized, i.e., created for reasons of pride or recreation by the developers
- Monetized through in-app purchases of 1) permanent enhancements (e.g., unlocking game levels, removing advertising, acquiring premium app features), 2) expendable or virtual goods (e.g., extra lives for game character), or 3) subscriptions (e.g., New York Times). As with app purchases, a share may go to the app store owner (e.g., 30% in the iOS case) [14].

Increasingly, however, apps are being monetized through collection and exploitation of information on the users, their equipment, location, and activities. This data is returned to the developer through the app store or directly through the macro infrastructure, and subsequently used to further their own business purposes or sold to a third party for targeted advertising.

The costs to develop an app are difficult to estimate and vary widely based on the complexity of the app. Given that the developer has the basic concept, the following provides some estimates for iPhone app programming costs [15]:

- Simple, table-based app - $1,000 - $4,000
- Database-driven app (native) - $8,000-$50,000
- Games - $10,000 - $250,000

Additional features such as in-app purchasing, using web services, game center interfaces, or other external interfaces would add additional costs. The app design, or the images and icons, will add $500 – $10,000 for a basic iPhone, with additional costs of 25% for iPhone 4 and 50% for iPad. The phenomenally successful Angry Birds game was developed by the Finnish company Rovio for approximately, $140,000 [16], with 1.7 billion game downloads, 263 million active users and 2012 sales of $195M including related merchandising [17].

3 DoD Requirements and Challenges

The DoD environment at the tactical edge and the reach-back to the major DoD facilities through its Global Information Grid (GIG) has both similarities and significant differences from the commercial counterparts. The DoD mobile apps ecosystem, which exists in tandem with the commercial ecosystem, is shown in Figure 3. The DoD version of the micro environment is similar, but this may cause one to underestimate the difficulties of the interactions with the macro environment.

A. DoD Challenges

Complexity of Software Applications. The complexity of DoD software initiatives varies widely across classes [7]:

- *Transformation apps* are built to take advantage of current opportunities and have a short life-cycle. They are often characterized by ad hoc processes and loose governance.
- *Differentiation apps and programs*, often external-facing, are built to support collaboration.
- *Core programs* support the critical organizational activities and data.

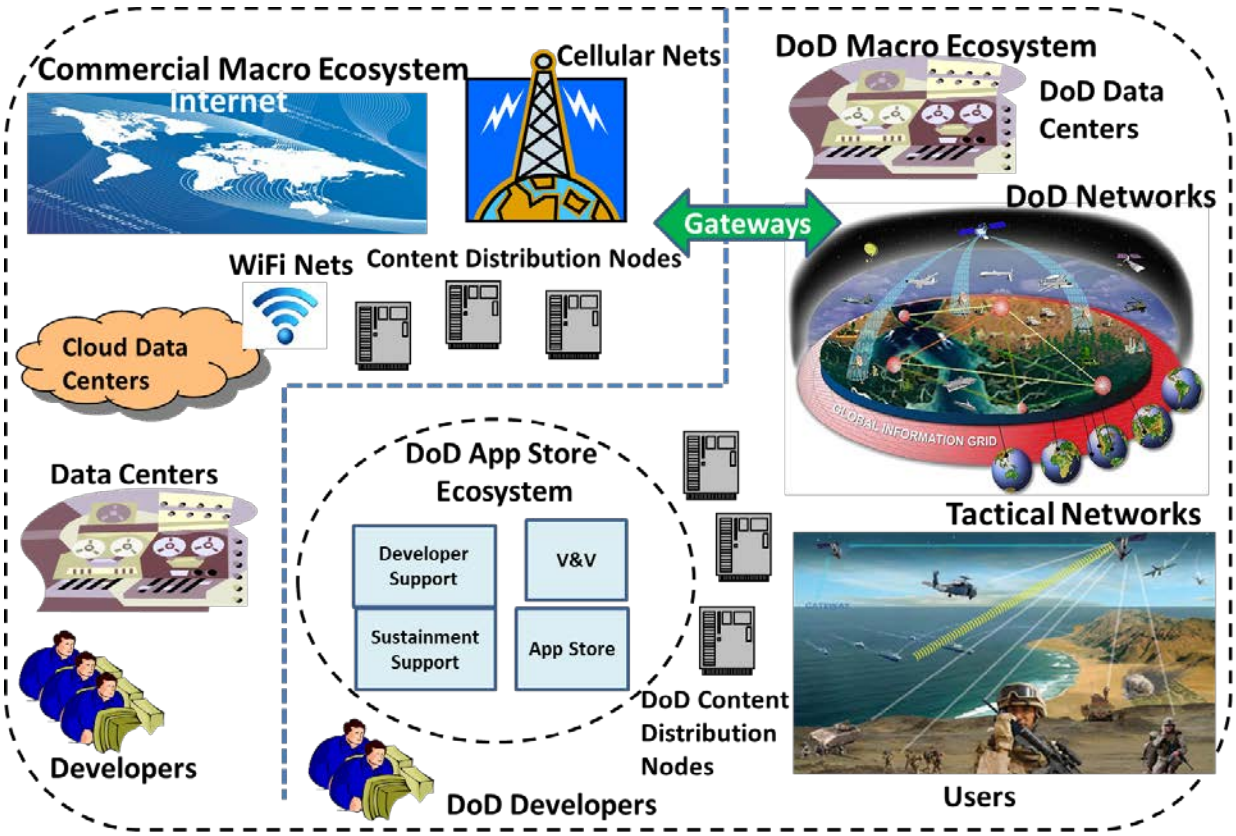


Figure 3: The DoD Mobile App Ecosystem

The transformative apps align well with many typical commercial mobile apps, and the differentiation apps and programs can readily leverage commercial mobile apps. However, the core programs require a rigorous software systems engineering discipline and strong governance.

Software Development Practices. The interactions between the developers and DoD will require DoD to change the way it approaches software development. The DoD has traditionally developed large, vertically integrated software systems to support its missions—such as command and control—using traditional, time consuming development processes. Interoperability between these systems is often problematic due to their long-life and complexity. On the commercial mobile application side, development is user driven and aimed at producing small, relatively simple applications that integrate a few functions, but generally do not integrate across a wide variety of functions, relying on the user to integrate.

Tactical Edge Communications Constraints. The communication infrastructure at the tactical edge is characterized as a DIL environment. There are bandwidth limitations due to the tactical land- and satellite-wireless networks, mobility needs, and the possibility of kinetic and cyber attack, which can result in users being unable to establish connections for unpredictable periods of time. The apps themselves should be cognizant of the network conditions to continue operating during disconnections.

HTML5 is seen as one method to help deal with the DIL environment. Another approach is to deploy content distribution nodes in strategic locations on the tactical networks to perform some of the remote processing and cache more frequently accessed data; however, this is currently a research topic.

Currently, there are only a few experimental end-devices employed at the tactical edge, so the platform choices are limited. Most DoD experiments to date are using Android-based smart-phones and tablets due to Android's open-source policy [18]. These devices are often tethered to standard military tactical radios or are interconnected in mobile local-area networks using hardened commercial technologies.

Security Requirements and Implications. There are obvious safety and security reasons to limit the collection of data on soldiers by apps to prevent the data being monitored or exfiltrated by a hostile agent. However, there are also many potentially beneficial reasons for DoD mobile apps to collect information from the users, such as using soldiers as sensors to develop situation awareness and to support various data mining activities. For example, the commercial app WAZE [19] is a community based traffic and navigation app that employs user feedback to collect real-time information on road conditions, speed cameras, gas stations, etc.[1]

The verification or validation (V&V) process (vetting) for the DoD is more complex than for commercial apps and involves extensive testing to: 1) make sure the apps are secure and not vulnerable to cyber-attacks (such as malware), tampering, or intercept, and 2) guaranteeing properties such as privacy, integrity, and non-repudiation in many cases. The effort required to properly vet the applications would be an expensive and time-consuming process for the DoD.

The DoD authentication needs are also more restrictive than those in the commercial world. A preferred authentication method is through the Common Access Card (CAC), a certificate-based, two-factor scheme which requires interoperation with the DoD PKI infrastructure. Sleeves or card-readers that attach to smart-phones are cumbersome and expensive and not well suited to the battlefield, so that some alternative authentication mechanisms are needed. There have been several SIM-card approaches proposed that may fill this need in the coming years[20].

The mobile devices issued to DoD personnel are typically managed using a Mobile Device Management (MDM) system for the enterprise users [21][22]. An MDM needs to be aware of the app store and app interactions and requirements, as well as enforce the security policies on the devices. It serves as a protected gateway between the mobile users and enterprise resources and monitors the devices and systems for security problems. Requirements and implementation details for an MDM that operates at the tactical edge have not been formalized or released.

Lack of a "Crowd"—in terms of both users and developers—to populate the App Store. As recently noted by Gartner in a discussion concerning enterprise app stores, "The primary determinant of success is app supply" [23]. In the DoD space, app supply stands to be a major issue. There is no mass market for

[1] In June 2013, Google purchase WAZE, an Isreali-based company for just under a billion dollars and has integrated its functions with their Google Maps web application and app. http://www.cnet.com/news/google-reveals-it-spent-966-million-in-waze-acquisition/

sales or the collection of data. The challenge for the DoD is how to incentivize app developers without this market. The DoD has 1.4 million active duty service members, 1.1 million in the National Guard and Reserves, and an additional 718,000 civilians. Comparing this number of users with the numbers shown in Table 1, it is not reasonable for the DoD to adopt a crowd-based model for the app developers without additional incentives.

B. DoD Pilot Experiments

In 2010, an early step toward an app store for the DoD was taken. A competition, called Apps for the Army (A4A), was held, and 53 apps were developed and submitted within 75 days. After a rapid vetting and judging process, 25 of the apps were selected and made available on a pilot app store known as the DoD Storefront. Some issues encountered during the experiment were: 1) more than 50% of the apps failed test and certification, 2) legal review took a long time, and 3) the DoD cloud environment had some problems [7]. In March 2012, the Army launched a new app store—the Army Software Marketplace—which was an Army web site listing apps that could be downloaded to an iPhone via iTunes [24]. There were only 25 apps—several dating back to the 2010 A4A competition—in Marketplace: 7 doctrine and publications, 4 training, 4 geospatial solutions, and 10 others. Clearly, app supply is a major issue.

Another effort, called Transformative Apps, was launched by DARPA in 2010 to investigate issues with providing apps to the warfighter [25]. The areas of interest include an apps marketplace architecture, apps development, middleware services and libraries, and network infrastructure. As part of the program, a secure host version of the Android-OS (version 2.2) was developed that also included data authentication and integrity checks [26]. Developers were contracted for apps to allow soldiers to load images and data on their mobile device, provide a map app for location of fellow soldiers, provide assistance in identifying explosives and weapons, and help in navigating parachute drops. Soldiers have also developed several apps to download map data, and a search and rescue app. DARPA is continuing investigation of apps that run in disconnected mode, fully interconnecting the devices, providing more robust links to the rear areas and better synchronization and back-up of data [26][27].

In a recent report [28], the DoD Inspector General (IG) found that the Army's adoption and use of Commercial Mobile Devices (CMDs)—purchased under pilot and non-pilot-programs—had outpaced the Army CIO's ability to define and implement policies to effectively manage the devices. The IG listed a number of deficiencies in several areas, including managing the device configurations (e.g., no MDM at some sites), sanitizing (e.g., remotely wiping) lost or stolen devices, and controlling the storage of sensitive data on the devices.

Several other DoD Components, including the other Military Services, DISA, and NSA, have launched mobility pilots over the past few years. DoD policy is beginning to catch up to usage of CMDs. In May 2012, the DoD CIO issued the DoD Mobile Device Strategy [21] and followed up with a DoD Implementation Plan [22]. The Plan, issued in February 2013, states that the Army app store, DARPA pilots, and several other pilots, some unclassified and others classified, will inform the current effort to bring mobility to the DoD enterprise.

DISA has moved forward with implementation of the plan and has begun to offer an enterprise MDM service since February 2014 for unclassified activities. A version to handle classified applications for mobile users is reportedly under development. The DoD has traditionally only approved Blackberry user devices due to their security architecture. More recently, several other devices and operating systems, including several versions of Android and iOS devices, have been approved via Secure Technical Implementation Guides (STIGs) for use with their MDM service [29]. The initial release capabilities of the MDM service includes a mobile application store, approved devices list, the mobile device management system, supported cellular access, DOD PKI support, access to DOD Enterprise Email, and access to the DOD Global Address List. The App store contains 16 mobile applications and an additional 90 apps area being vetted. The service hopes to expand to 100,000 users in increments of 25,000 by the end of 2014 [30]. Recent pilot programs by the services show heightened interest in using Android and iOS based phones and tablets with the new service. For example, the Air Force recently decided to replace 5000 Blackberry devices with Apple iOS 6 devices [31].

C. Strategies for DoD App Development

The question of what strategy should be employed to best develop the DoD apps ecosystem is still open. One approach is to determine the most common uses of mobile devices on the commercial side and then reflect these on the tactical side with suitable modifications. In Table 2, the top ten activities are given for commercial smart phones and tablets [32]. A generic military activity that could use this functionality is identified. The activities that have proven their value to users are the best candidates to be developed and deployed first.

Table 2: Common Usage and Military Analogs [27]

Fraction of Users Who Engaged in Activity[a]			**Tactical Edge Applicability**
Activity	***Smartphone***[b]	***Tablet***[b]	
Sent text message to phone	90.50%	*	Command, Control, and Communications (C3)
Took photos	83.40%	*	Intelligence, Surveillance, Reconnaissance (ISR)
Used email	77.80%	73.60%	C3
Accessed weather	67.10%	64.60%	Situation Awareness
Accessed social networking	65.30%	67.50%	Collaboration
Accessed search	58.70%	73.90%	Situation Awareness
Played games	52.90%	66.30%	Training
Accessed maps	51.20%	*	Situation Awareness
Accessed news	49.20%	58.80%	Situation Awareness
Listened to music on phone	48.00%	*	Training
Accessed photo/video sharing site	*	51.50%	ISR
Read books	*	51.20%	Training
Watched video	*	50.90%	ISR; Training
Accessed retail	*	49.80%	Logistics

[a] During a 3-month period ending December 2012

[b] Asterisk indicates that activity was not a Top 10 Activity for specified user population

4 Research Areas

Technological advances are needed to adapt apps to the tactical mobile ad hoc networks (MANETs) that will be deployed on the battlefield in the near future. Security concerns still need to be addressed for the tactical environment, including communications with allies and other coalition partners. Recent work by the NSA has demonstrated the ability to have a secure conversation using modified commercial devices, which may eventually be employable in the battlefield [33]. DARPA is investigating Content-based Mobile Edge Networking (CBMEN) for mobile ad hoc networks [34][35]. The specific goals include minimizing reach-back, latency, and transparently locating, distributing, and sharing battlefield content. Although not directly targeted at mobile apps, improvements developed in CBMEN will be applicable to mobile app deployments.

An obvious approach to supplying apps to the tactical edge is through customization of existing commercial apps. However, this customization must be done in such a way as to be able to keep up with the rapid product cycles of the commercial world. One method, called Modified-off-the shelf (MOTS) [1], proposes a modular approach that minimizes the code changes, still requires research and development in software engineering of mobile apps to define the best principles and practices.

5 Conclusion

The temptation to tap into the seemingly unending flow of new apps for mobile devices will increase from the perspective of the soldiers at the tactical edge. Technical barriers such as DIL communications will need to be mitigated with cognizant apps and new content distribution methods in order for these to be successfully deployed at the edge.

A large part of the success of the mobile apps in the commercial world is due to the existence of both the micro and macro ecosystems. The market drivers for the DoD will never match those of the commercial environment. Simply providing a DoD version of the micro ecosystem in the form of a DoD app store is not sufficient. Novel incentives for developers, as well as investment in new development approaches, such as MOTS, that can adapt the commercial apps are needed. Failure to address these issues will continue to result in disappointing results, limited supply, and slow adoption of mobile apps at the tactical edge. In addition, many successful commercial apps are windows into valuable and useful data sites; the DoD needs to make more of its data sources available and accessible so that apps can deliver the data to the warfighters in useful forms and achieve the goals of net-centric operation and shared awareness.

Acknowledgment

This work was performed under Institute for Defense Analyses Contract No. W91WAW-11-C-0047, task order AK-2-3474.

References

[1] J.R. Agre, K.D. Gordon, and M.S. Vassiliou, "Commercial technology at the tactical edge," 18th ICCRTS, 19-21 June 2013, in press.

[2] IDC, "More smartphones were shipped in Q1 2013 than feature phones, An industry first according to IDC," 25 April 2013.

[3] D. Rowinski, "Google Play Hits One Million Android Apps," ReadWrite, 24 July 2013.

[4] Apple, Inc., "Apple Announces iPad Air—Dramatically Thinner, Lighter & More Powerful iPad," Press Release, 22 October 2013.

[5] Steel Media Ventures, "App Store Metrics," 148Apps.biz, 6 May 2014.

[6] Apple, Inc., "iTunes Charts: Free Apps," 10 May 2014.

[7] Seeking Alpha, "Apple's CEO Discusses F2Q 2014 Results - Earnings Call Transcript," Apr. 23, 2014.

[8] C. Wortman, "Army Software Transformation: How We Accelerate Software Capabilities to the Field," Briefing, Army CIO/G-6 Advisory Panel Meeting, 10 November 2010.

[9] J.S. Hammond and J.A. Ask, The Future Of mobile application development, Forrester Research, Inc., 17 January 2013.

[10] ABI Research, "1.4 billion HTML5-capable mobile devices in 2013, but developer uptake requires stronger OS, chipset integration, says ABI research," Business Wire, 9 April 2013.

[11] N. Ingraham, "Apple announces 1 million apps in the App Store, more than 1 billion songs played on iTunes radio," The Verge, VOX Media, Inc., 22 October 2013.

[12] M. Rogowsky, "Without Much Fanfare, Apple Has Sold Its 500 Millionth iPhone," Forbes.com, 25 March 2014.

[13] C. Zibreg, "Apple has 2x or more credit cards on file than Amazon," iDownloadBlog, 28 April 2014.

[14] Apple Inc, https://developer.apple.com/programs/ios/.

[15] C. Thomas, "How much does it cost to develop an app," bluecloud solutions, 2013.

[16] T. Cheshire, "In depth: How Rovio made Angry Birds a winner (and what's next)," Wired Magazine, March 7, 2011.

[17] I. Lunden, "Sales Up 101% to $195M with merchandising, IP 45% of that; net profit $71M," TechCrunch, April 3, 2013.

[18] L. Stoker, "Battlefield smartphones receive a ringing endorsement," ArmyTechnology.com, 31 July 2012.

[19] WAZE Inc, www.waze.com

[20] Koolspan Inc., www.koolspan.com.

[21] DoD CIO, Department of Defense Mobile Device Strategy, Version 2.0, May 2012.

[22] DoD CIO Memorandum, Department of Defense Commercial Mobile Device Implementation Plan, 15 February 2013.

[23] Gartner, Inc., "Gartner says that by 2017, 25 percent of enterprises will have an enterprise app store," press release, 12 February 2013.

[24] Army CIO/G-6, "Army launches apps marketplace prototype," 23 March 2012.

[25] DARPA, Transformative Apps, FedBizOps, DARPA-BAA-10-41, 3 March 2010.

[26] H. Kenyon "Thank DARPA for hardened Android OS," Defense Systems, 31 January 2012.

[27] S.E. Ante, "Military takes apps to war," *online.wsj.com*, 4 September 2012.

[28] DoD Inspector General, Improvements needed with tracking and configuring Army commercial mobile devices, DODIG-2013-060, 26 March 2013.

[29] DISA, Mobile Devices and Wireless Services

[30] J. Cheng, "DoDs Mobility Plan a Boon for Blackberry," Defense Systems, Jan. 21, 2014,

[31] J. Cheng, "Air Force to swap 5000 Blackberrys for iOS Devices," Defense Systems, Feb. 20, 2014.

[32] comScore, Inc., 2013 Mobile Future in Focus, February 2013.

[33] B. Iannota, "Top Secret Goes Mobile," Defense News, 29 March 2012.

[34] DARPA, Content-Based Mobile Edge Networking (CBMEN), FedBizOps, DARPA-BAA-11-51, 26 April 2011.
[35] K. Gremban, Content-Based Mobile Edge Networking (CBMEN): DARPA-BAA 11-51, Proposers' Day Presentation, 13 May 2011.

IDA

Institute for Defense Analyses

4850 Mark Center Drive • Alexandria, Virginia 22311-1882

Practical Considerations for Use of Mobile Apps at the Tactical Edge

19th ICCRTS

June 17, 2014

Jonathan Agre, Karen Gordon, Marius Vassiliou

Institute for Defense Analyses

Summary of Main Points

- DoD has strong interest in using mobile electronics and mobile apps at the tactical edge
  - Multi-function, size, weight, power
- Desire to take advantage of rich Mobile App environment
- Simple adoption of commercial apps at tactical edge is not feasible due to technical and market differences in the ecosystems
- Changes are needed in software development practice, customization, communications infrastructure, design of Apps, and deployment of Apps

Overview

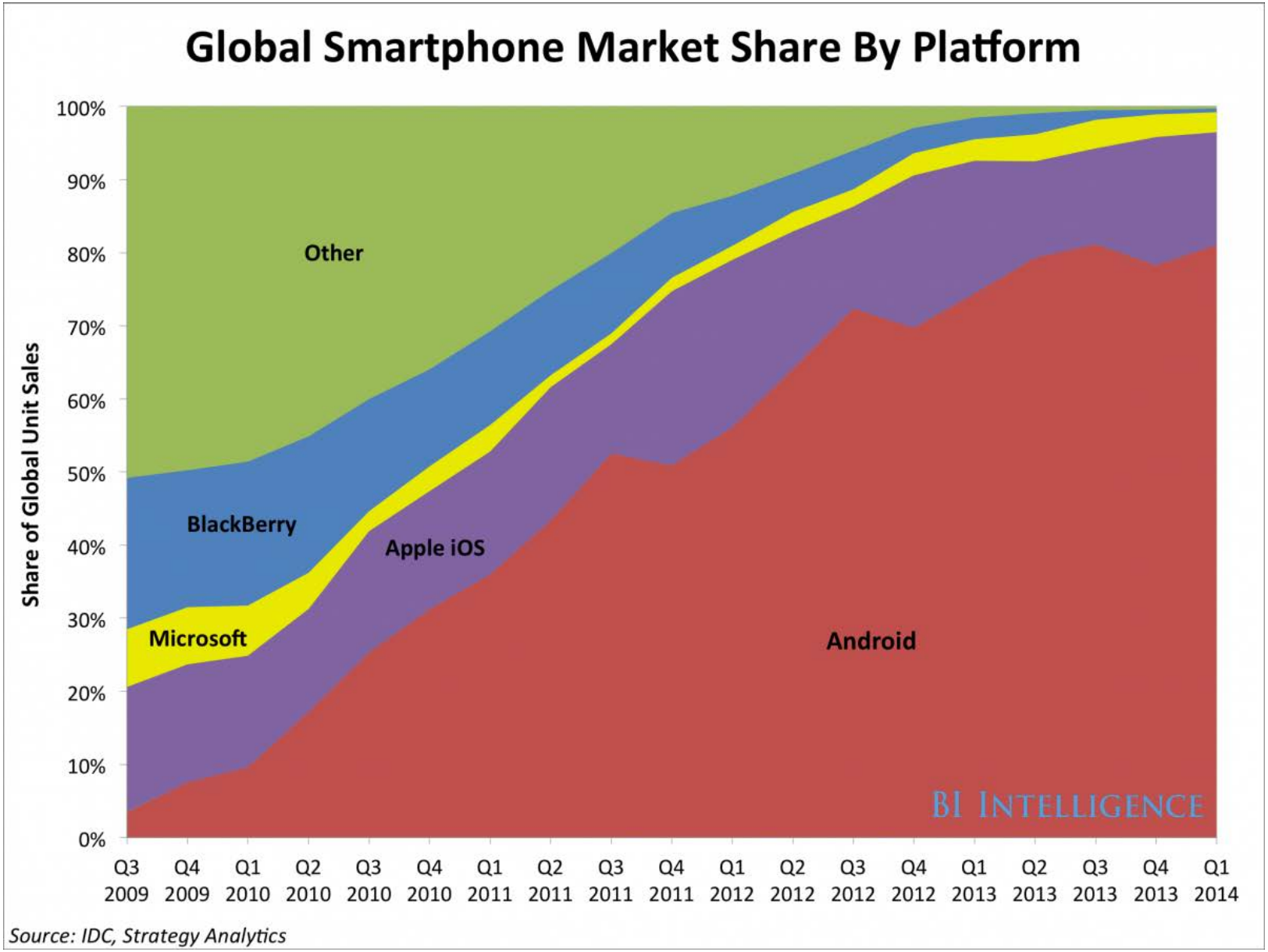
- Mobile App Mass Market
- Commercial Mobile App Ecosystem
- DoD Mobile App Environment
- Challenges for DoD Mobile Apps
- Recent efforts at DoD
- Identification of Areas for Further R&D
- Conclusions

IDA | Mass Market for Mobile Apps

- Increasing use of smart mobile electronics
  - In 2013 more smart phones sold than conventional phones
- Huge market in Apps for mobile electronics
  - 2013 - Global revenue from app stores is expected to rise 62% this year to $25 billion, according to Gartner

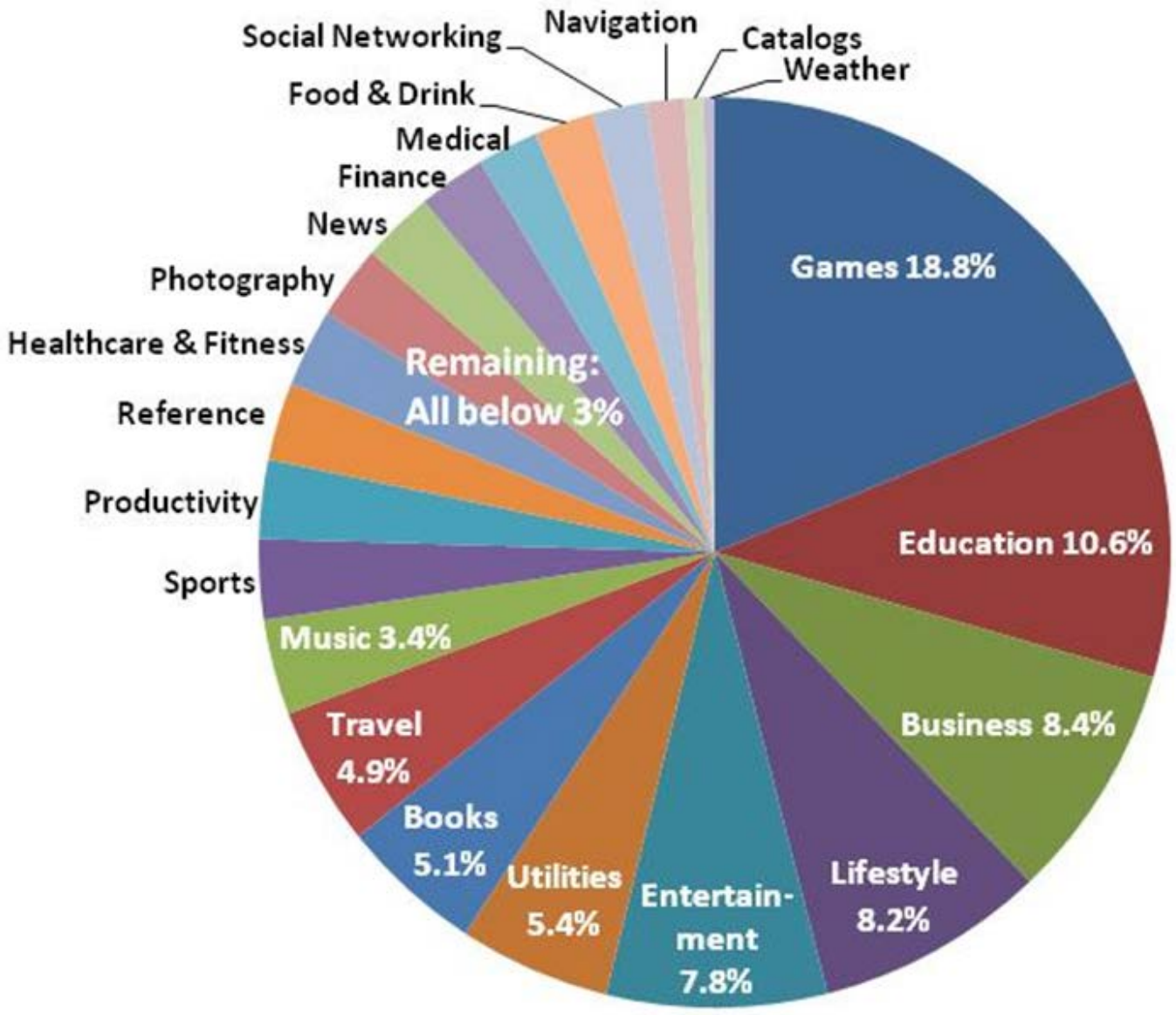
iPhones sold	500 million
iOS devices sold	800 million
Active iTunes accounts	800 million
Countries represented	155
Active iOS apps	1.1 million
iOS downloads	60 billion
Registered iOS developers	300,000
Payments to iOS developers	$13 billion

IDA



http://www.businessinsider.com/iphone-v-android-market-share-2014-5

Categories of Mobile Apps in iTunes App Store



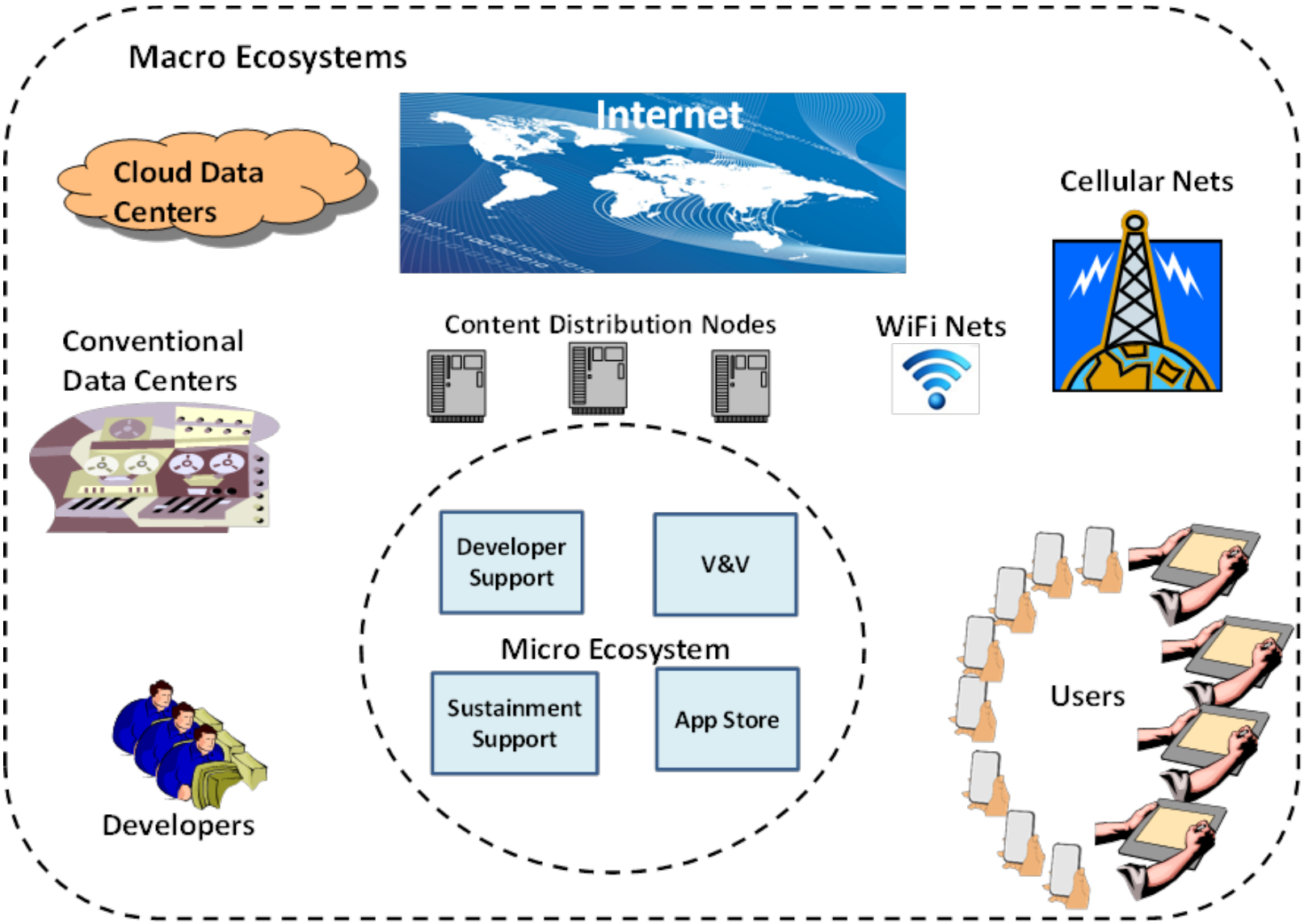
IDA | Common Usage and Military Analogs

Fraction of Users Who Engaged in Activity			Tactical Edge Applicability
Activity	Smartphone	Tablet	
Sent text message to phone	90.50%	*	Command, Control, and Communications (C3)
Took photos	83.40%	*	Intelligence, Surveillance, Reconnaissance (ISR)
Used email	77.80%	73.60%	C3
Accessed weather	67.10%	64.60%	Situation Awareness
Accessed social networking	65.30%	67.50%	Collaboration
Accessed search	58.70%	73.90%	Situation Awareness
Played games	52.90%	66.30%	Training
Accessed maps	51.20%	*	Situation Awareness
Accessed news	49.20%	58.80%	Situation Awareness
Listened to music on phone	48.00%	*	Training
Accessed photo/video sharing site	*	51.50%	ISR
Read books	*	51.20%	Training
Watched video	*	50.90%	ISR; Training
Accessed retail	*	49.80%	Logistics

IDA | Military Capabilities and Commercial Apps

Military Capability	Similar Commercial Smartphone/Tablet Apps
Command and Control	Chat/IM, SMS, MMS, voice call, video call, Twitter, email, Skype
Mission Planning and Execution	Electronic Flight Bag
Situation Awareness (Blue Force Tracking)	WAZE, Google Maps/Earth, StarChart, Location-based Apps, News feeds
Streaming Video	YouTube, Hulu, Crackle
ISR	Home Monitoring, Friends Tracking, Picture tagging
Soldier as a Sensor	WAZE, Ratings
Biometrics	Face, Voice, Keystroke, IRIS Recognition, fingerprint matching, browsers
Secure, Hands-Free Communications	WICKR, Speech-to-text, Siri
Information Sharing, Access	Dropbox, browsers, Splashtop Whiteboard
Document and Media Exploitation (DOMEX)	Google Translate, iTranslate, Mobile OCR
Education, Training	YouTube, Wikipedia, Dictionary,
Personal applications	Alerts, financial, social media, shopping, games, etc

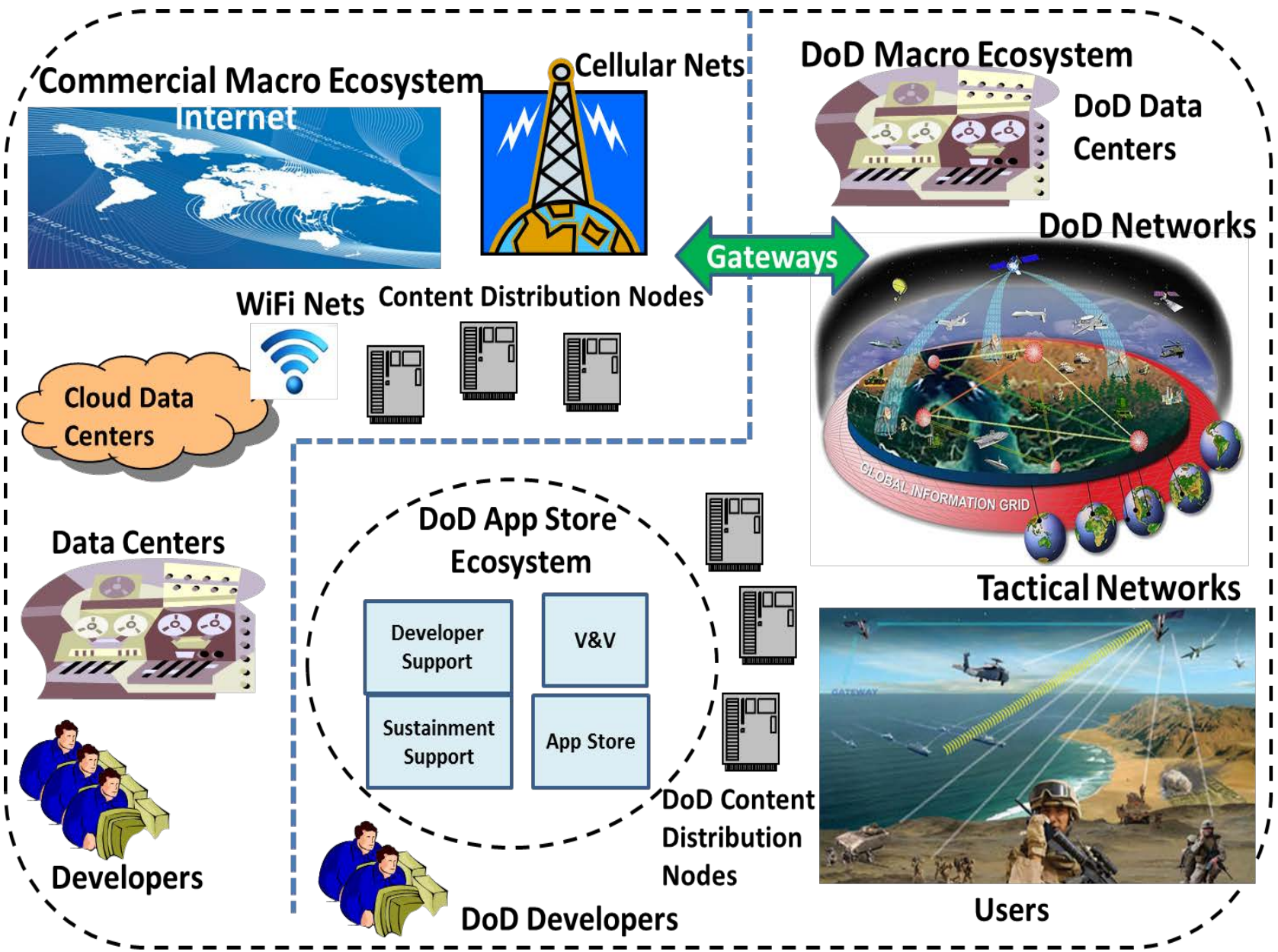
IDA | Commercial Mobile Apps Ecosystem



Main Functions of App Store Deployment

- Interact with App Store App
- Secure efficient hosting of Apps
- Identification of user platforms, correct versions
- Efficient downloads
- Authentication and access control
- Attestation of the Apps
- Support for updates and maintenance functions
- Support for upgrades
- Display of Apps, ratings, search
- Support for accounting functions – payments
- Deliver user data to developer – activities, location…

IDA | DoD Mobile App Environment



Comparison of DoD and Commercial App Ecosystem

	Commercial	DoD
Complexity of Application	Low, single function	Low to High (integrated functions)
Software Development	Rapid, Evolutionary, User Driven	Traditional, slow, requirements driven
Communication Environment	Robust, high data rates	Disconnected, intermittent, Limited
V&V	Basic, App store provided	Complex, DoD provided
Security/Access Control	Basic	Mission critical
Privacy	Basic, Developer controlled	Critical, DoD controlled
Developer Motivation	70% of sales	Contract
Crowd-based feedback	High (>1 Billion users)	Low (< 3 Million users in all DoD)
Monetization	In-App, Selling data	None

IDA | Recent DoD Activities

- 2010 Apps4Army
  - 53 Apps submitted, 25 vetted and made available on DoD Storefront
  - 50% failed certification, legal review was long, DoD Cloud had problems
- 2010 DARPA Transformative Apps Project
  - App Store Architecture, Middleware, Secure Android
- 2012 New Army Software Marketplace
  - Listed 25 Apps iTunes on App store (some from Apps4Army)
- 2012 DOD CIO – Mobile Device Strategy and Implementation Plan (2013) includes enterprise App Store
- 2014 DISA – Offer enterprise MDM service (unclassified)
  - Allows Android and iOS phones in addition to Blackberry
  - Includes support for App Store, PKI, directory and email
  - App store currently has 16 Apps

- Motivate, sustain developers for supporting DoD ecosystem
- Apps adapted to DIL networks and for Mobile Ad Hoc Networks
- Methods to reduce reachback
  - Content Delivery Nodes at tactical edge (DARPA)
  - Other forms of edge processing
- Secure Conversations over mobile devices (NSA)
- Methods to modify COTS software
  - Modified off the shelf (MOTS) software development to keep up with product cycles

Conclusions

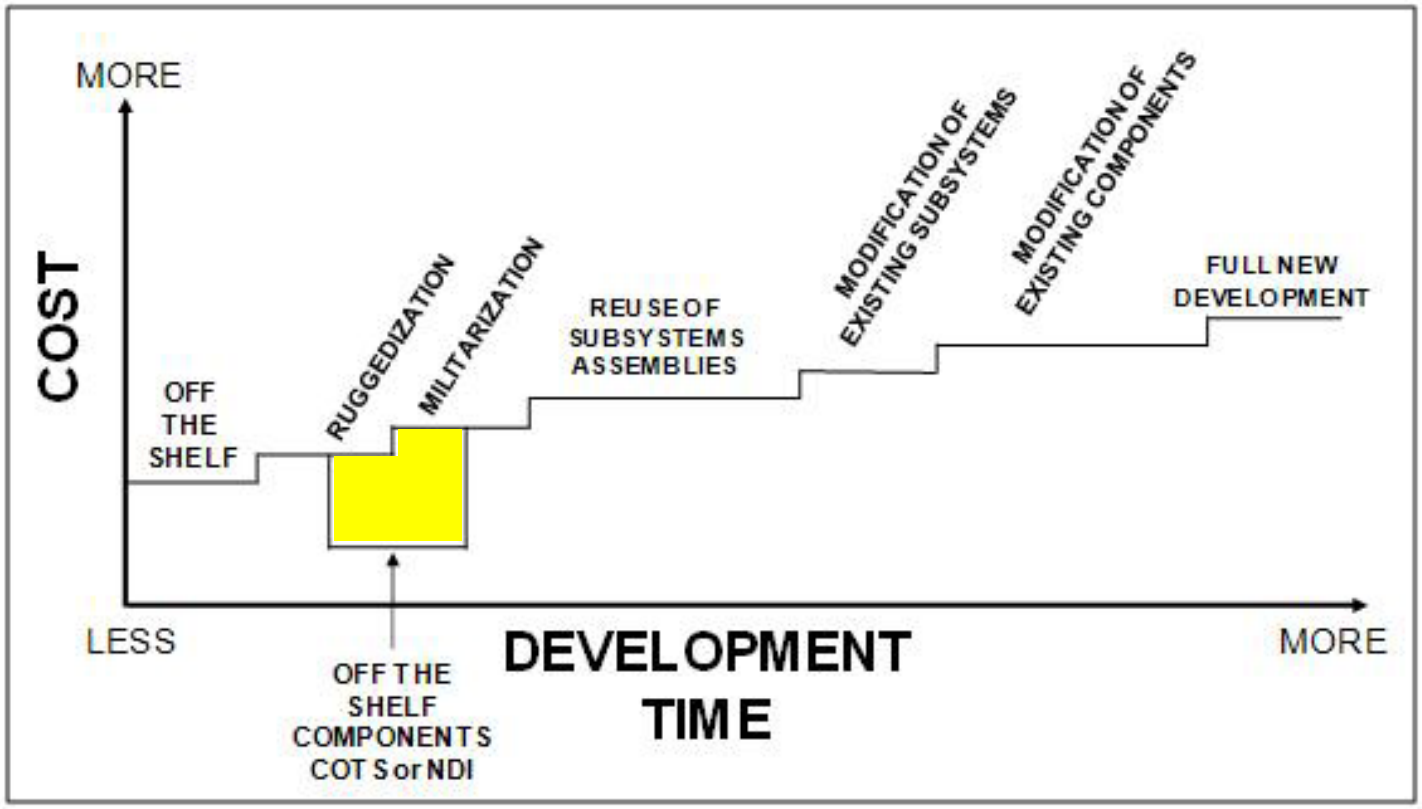
- DoD has strong interest in using mobile electronics and mobile apps at the tactical edge
  - Multi-function, Size, weight, power
- Desire to take advantage of rich mobile App environment
- Simple adoption of commercial apps at tactical edge is not feasible due to technical and market differences in the ecosystems
- Changes are needed in software development practice and customization, communications infrastructure, design of Apps, deployment of Apps

Further R&D is needed to leverage commercial Mobile Apps to increasingly realize goals of Net-Centric operations

IDA

Backup

Spectrum of Development Strategies



MOTS – Modified-off-the-shelf

Modifications to COTS for military purposes that retains ability to keep up with COTS product evolution

Source: Test & Evaluation Management Guide, Sixth Edition, US DoD, December, 2012, Chap 23

IDA | Issues with COTS and the Tactical Edge

Interoperability/Integration	With the IP-based GIG and with existing tactical network equipment – JTRS, WIN-T (JNN) and WIN-T INC 2
Disconnected, Intermittent, and Limited (DIL) Communications	Delay Tolerance
	Mobile Ad Hoc Networks (MANETs)
	Loss of infrastructure
Security	Cyber Offense/Defense methods
	Encryption for data at rest/data in transit
	LPI/LPD, Antijam, Anti-spoof
	Authentication – 2 factor, biometrics
	Cross domain
	Patching
Environmental Factors	Rugged, water proof
	User interface -sun glare, night vision mode, low light, touchable with glove
Acquisition	Supply-chain considerations
Network Operations and Management	Spectrum
	AAA
	Monitoring, Remote auditing
	Loss of infrastructure
	Capture of equipment (remote wipe)
	Remote peripheral control
Size, Weight, and Power (SWAP) Constraints	Power requirements, battery life, battery type
	Portability
App Management	App ecosystem

Selected R&D Areas That Can Impact Tactical Networks

- Software Defined Networking (SDN)
- Autonomic Networks (ANs)and Self Organizing Networks (SONs)
- Cognitive radio – spectrum sharing
- Hands-free operation
  - Face recognition, gesture-based inputs, speech recognition
- Software engineering methods to address MOTS

MOTS Example: Samsung Evolution Kit TV

Replace modular box to upgrade TV